Bureau of Alcohol, Tobacco, Firearms & Explosives

Privacy Impact Assessment
for
National Field Office Case Information System (NFOCIS)

Issued by:
Adam C. Siple
Chief, Disclosure Division &
Senior Component Official for Privacy

Approved by: Peter Winn, Acting Chief Privacy and Civil Liberties Officer, Department of Justice

Date approved: September 18, 2019]

(May 2015 DOJ PIA Form)

EXECUTIVE SUMMARY

The National Field Office Case Information System (NFOCIS) is the case management system and database that the Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF or "the Bureau") uses to create, track, and collect investigative information in support of ATF's law enforcement mission, strategic goals, program initiatives, and tactical field activities. NFOCIS serves many purposes, including but not limited to the following:

a. NFOCIS provides Special Agents, Industry Operations Investigators (IOIs)[1], and persons assigned to investigations the ability to post data to tables in a central database repository on a single server that is accessed through the NFOCIS applications.
b. The NFOCIS applications provide field managers and supervisors with management reports and query tools to drill down into data stored in the NFOCIS database in order to measure office, field division, program, and individual performance.
c. The NFOCIS Branch provides Headquarters program offices with queries to measure and report on the performance of program initiatives.
d. The NFOCIS Branch provides ATF's Budget Office with reports and data that can be reported to ATF's stakeholders, oversight entities (Office of Management and Budget (OMB), the Government Accountability Office (GAO) and Congress), and the public.

The original NFOCIS Privacy Impact Assessment (PIA) was published on May 31, 2006. ATF is updating the NFOCIS PIA based on an Office of the Inspector General audit recommendation. NFOCIS collects, maintains, and shares personally identifiable information (PII) on law enforcement officials and members of the public. NFOCIS is privacy sensitive due to the amount of information that may be collected in response to a law enforcement investigation or regulatory inspection. Due to the nature of criminal law enforcement investigations, ATF may collect, maintain, or disseminate information that is not a structured field, but is relevant and necessary to the investigation.

Section 1: Description of the Information System

Provide a non-technical overall description of the system that addresses:

(a) the purpose(s) that the records and/or system are designed to serve;
(b) the way the system operates to achieve the purpose(s);
(c) the type of information collected, maintained, used, or disseminated by the system;
(d) who has access to information in the system;
(e) how information in the system is retrieved by the user;
(f) how information is transmitted to and from the system;
(g) whether it is a standalone system or interconnects with other systems (identifying and

[1] An Industry Operations Investigator conducts investigations and inspections designed to carry out the Federal government's regulatory responsibilities pertaining to the firearms and explosives industries. *See* Bureau of Alcohol, Tobacco, Firearms & Explosives, *Fact Sheet - Industry Operations Investigator (IOI)* https://www.atf.gov/resource-center/fact-sheet/fact-sheet-industry-operations-investigator-ioi (last visited June 27, 2019).

describing any other systems to which it interconnects); and
(h) whether it is a general support system, major application, or other type of system.

NFOCIS is the case management system and database ATF uses to create, track, and collect investigative information in support of ATF's law enforcement mission, strategic goals, program initiatives, and tactical field activities. NFOCIS is a major application used by agents, investigators, and analysts throughout ATF.

NFOCIS is comprised of a suite of integrated case management applications that meet the unique business requirements of multiple ATF end users. It allows Special Agents, IOIs, and persons assigned to investigations to post data to tables in a central database repository on a single server that is accessed through the system applications. The program is client based and therefore any inputted data is transmitted through a secure Virtual Private Network (VPN).[2]

NFOCIS interconnects with a limited number of systems that includes the Electronic Tracing (eTrace) system, the Bomb, Arson, Tracking System (BATS), Semantica Pro, and the ATF National Instant Background Check System Referral (ANR) information system.[3]

- The eTrace system is a web-based application developed to provide web-based firearm trace submission and analysis capabilities to ATF, domestic, and foreign law enforcement agencies. eTrace allows users the ability to electronically submit firearm trace requests, to monitor the progress of traces, to retrieve completed trace results, and to query firearm trace-related data in a real-time environment. The system not only provides registered users with the ability to electronically submit firearm trace requests, it also allows them to monitor the progress of these traces.
- BATS is a web-based system that facilitates and promotes the collection, sharing and diffusion of intelligence information concerning fires, arsons, and the criminal misuse of explosives.
- The Semantica Pro system is an analysis tool that enables users to access information from existing ATF and commercial databases (without altering the data in the original database) and to perform intelligence analysis, fuse, and visualize data for use in criminal and regulatory investigations.
- The ANR information system was developed in order to allow users to receive and process firearm denial[4] information and firearm retrieval notifications received from the Federal Bureau of Investigation (FBI). The ANR system captures the determination of whether the firearm transfer (for example, the sale of a firearm) would violate Federal, State or local laws and issues

[2] A "Virtual Private Network" is a virtual network built on top of existing networks that can provide a secure communications mechanism for data and Internet Protocol information transmitted between networks. National Institute of Standards and Technology, Special Publication 800-77, *Guide to IPsec VPNs* (Dec. 2005).
[3] These interconnected systems are covered by separate privacy documentation, as necessary and appropriate.
[4] There are two kinds of denials. Standard denials are those that were denied before the end of the third full business day from the date of the initial National Instant Criminal Background Check System (NICS) check, and means that a dealer could not legally transfer the weapon. Delayed denials are those that were denied more than 3 full business days after the date of the initial NICS check processing, and therefore after the 3-day period during which the dealer is required to suspend the transfer. The dealer may or may not have transferred the firearm in such cases.

denials to applicants prohibited from purchasing firearms. ATF Denial Enforcement NICS Intelligence (DENI) Branch staff review any FBI comments associated with the denied transactions and verify criminal history data. They also may contact dealers to obtain copies of the application to purchase firearms (ATF Form 4473, Firearm Transfer Record). ATF DENI Branch staff also contacts judicial and law enforcement agencies to request copies of documentation to support or refute the FBI's decision to deny the firearm transfer, if necessary. Information maintained in these databases, if warranted, is then electronically transmitted to the NFOCIS system, creating a general case number for assignment to a case agent to investigate matters involving delayed denials.

NFOCIS provides field managers and supervisors, as well as Headquarters program offices, with queries and tools to analyze data in order to measure office, field division, program, and individual performance on program initiatives. Further, NFOCIS provides ATF's Budget Office with information and data that can be reported to ATF's stakeholders, oversight entities (e.g., OMB, GAO, and Congress), and the public.

In general, the system exploits information technology and develops, manages, and utilizes a centralized information repository, enabling ATF to collect, manage, analyze, and disseminate the Bureau's investigative, intelligence, and inspection information. The system and its applications collect and maintain PII as detailed in Section 2.1, below. Specific references relating to portions of the systems containing PII are designated "PII" within this document.

NFOCIS consists of four applications: (1) N-Force; (2) N-Spect; (3) N-Quire; and (4) N-Force Vault. These four applications are described in more detail below.

(1) N-Force is a computer-based case management system that supports ATF's law enforcement operations by providing automated collection, dissemination, management, and analysis of investigative data. N-Force is designed as a single-point of data entry system where case information is entered once and then used in multiple areas throughout the system. For each case, N-Force captures and reports on the following categories of data, detailed in Section 2, below:

- Who (persons, suspects, defendants, investigative participants – includes PII)
- What (events, property)
- Where (locations – includes PII)
- When (events)
- How (investigative techniques, narratives)
- Why (narratives)

N-Force also automatically generates and formats Reports of Investigation, which also contain PII. Access to the system is delineated as follows: Bureau wide, a user with an "Intelligence Officer" role can access the system on a READ ONLY basis. Generally speaking, all Special Agents in the field have "Intelligence Officer" access. Some supervisory Special Agents (i.e., Resident Agents in Charge and Special Agents in Charge) can only access cases within their assigned Group and/or Field

Divisions. Further, Special Agents in the field are given this right, as it is an investigative need to determine if cases are related to one another and/or to determine steps to deconflict investigative pursuits.

Other Job Series (such as Investigative Analysts (IA), Intelligence Research Specialists, etc.) may be granted "Intelligence Officer" access by their first line supervisor, as warranted by the scope of their position/work-function. Such requests must come from that supervisor to the NFOCIS mailbox.

It should be noted that the only type of case that cannot be accessed, no matter user class settings, are cases marked "Restricted." To access such cases, the designated Case Agent of the "Restricted" case must "manually" add "Participants" through the NFORCE application within that case.

(2) N-Spect is an inspection management system, which supports ATF's regulatory responsibilities related to the firearm and explosive industries. N-Spect and N-Force are independent applications with the NFOCIS suite and are not connected. N-Spect is designed to reduce the administrative burden on ATF investigators. For each inspection, N-Spect captures the following categories of information, detailed in Section 2, below:

- Location information (includes work-related PII)
- Inspection assignment information
- Inspection assignment results information
- Industry Member[5] information (includes PII)
- Violations information
- Recommendation information
- Referral information (includes PII)
- Inspection Documents (includes PII)
- Inspection Spreadsheets
- Person information (includes PII)
- Explosive information
- Investigative participant information (includes PII)
- Inspection documents and spreadsheets
- Related inspection information
- Post inspection information

Some of the documents listed above could contain tax information that is protected pursuant to the Internal Revenue Code, 26 U.S.C. § 6103. N-Spect automatically generates and formats reports regarding inspections.

NSPECT user role and user access are controlled through administrators who are the NSPECT program manager and NFOCIS analysts stationed in the NFOCIS group. Any NSPECT user/role has the

[5] An Industry Member can be a Federal Firearms Licensee (FFL), a Federal Explosive Licensee (FEL), or an employee under a FFL or FEL.

capability to access "closed" inspections within NSPECT and have read only view of all the information contained in the User Interface (UI). For open or active inspections, generally only the assigned IOI, Supervisor, Director of Industry Operations (DIO), DIO assistant, Division Counsel, or IA of that field office can view the information contained within an open UI. The IA, DIO, DIO assistant, and Supervisor are the only roles that can add additional assigned users to the case who can view and edit the information.

NSPECT has a couple user roles that allow a user to access any open UI in the system which are reserved for specific HQ personnel at a very limited basis based on specific need (e.g., Counsel, Monitored case Program Manager).

(3) N-Quire is a case management system designed to collect and analyze large volumes of information by concurrent users, create reports, and generate forms related to significant criminal investigations and command post operations. N-Quire utilizes the same central database repository mentioned in the N-Force summary above and provides analytical capabilities. Its intuitive "folder-based" user interface allows for easy navigation through the case information. The following information elements are captured and reported on in N-Quire, and detailed in Section 2, below:

- Crime Scene information
- Investigative Lead information (includes PII)
- Person/Suspect information (including judicial status and includes PII)
- Timeline Event information
- Business/Location information (includes PII)
- Vehicle information (includes PII)
- Investigative Participant information (includes PII)
- Organization information (includes PII)
- Evidence/Property information
- Insurance Policy information (includes PII)
- Financial Account information (includes PII and financial data)
- Financial Transaction information (includes PII and financial data)
- Loan information (includes PII and financial data)
- Credit Card information (includes PII and financial data)
- Retail Transaction information (includes PII)
- Reports of Investigation information (includes PII)
- Source Document Information (includes PII)

Access to the application is governed by a user's role and the type of access required for the performance of their work-function, as determined by their supervisor.

(4) N-Force Vault is a web-based property management system, used to track property items held in evidence vaults. N-Force vault access is restricted to ATF assigned vault custodians, group supervisors, and contractors only. The system captures user log-in and log-out times on the back end. This application enables users to check property items into a vault and check out items for disposition.

In addition, N-Force Vault facilitates regular vault inventories and generates management reports. For all property in custody, N-Force Vault provides the following capabilities:

- Logging In
- Searching for Property (includes scanned, basic, and advanced searches)
- Checking In Property
- Checking Out Property
- Checking Out Property in Batch
- Moving Property
- Reconciling the Vault
- Managing the Vault
- Generating Custody Reports (includes PII)
- Generating Inventory Reports
- Generating Management Reports
- Use of the PERCON Barcode Reader

Access to the application is governed by a user's role and the type of access required for the performance of their work-function, as determined by their supervisor.

Section 2: Information in the System

2.1 Indicate below what information is collected, maintained, or disseminated. (Check all that apply.)

Identifying numbers					
Social Security	X	Alien Registration	X	Financial account	X
Taxpayer ID	X	Driver's license	X	Financial transaction	X
Employee ID	X	Passport	X	Patient ID	X
File/case ID	X	Credit card	X		
Other identifying numbers (specify): Insurance policy number					

General personal data					
Name	X	Date of birth	X	Religion	
Maiden name	X	Place of birth	X	Financial info	X
Alias	X	Home address	X	Medical information	
Gender	X	Telephone number	X	Military service	
Age	X	Email address	X	Physical characteristics	X
Race/ethnicity	X	Education		Mother's maiden name	X

General personal data
Other general personal data (specify):

Work-related data					
Occupation	X	Telephone number	X	Salary	
Job title	X	Email address	X	Work history	
Work address	X	Business associates	X		
Other work-related data (specify):					

Distinguishing features/Biometrics					
Fingerprints	X	Photos	X	DNA profiles	
Palm prints		Scars, marks, tattoos	X	Retina/iris scans	
Voice recording/signatures	X	Vascular scan		Dental profile	
Other distinguishing features/biometrics (specify): In terms of collecting fingerprints, NFOCIS collects the National Crime Information Center number; however, the case agent may scan in the fingerprint card as a source document.					

System admin/audit data					
User ID	X	Date/time of access	X	ID files accessed	X
IP address	X	Queries run	X	Contents of files	X
Other system/audit data (specify):					

Other information (specify)
Gang affiliation, if applicable.
NOTE: The checked information above indicates the information that ATF collects, maintains, or disseminates in the NFOCIS system that is a structured field within the system. Due to the nature of criminal law enforcement investigations, ATF may collect, maintain, or disseminate information that is not a structured field, but is relevant and necessary to the investigation, such as religion (for example, when necessary and relevant to an arson involving a place of worship), education, medical information, etc.

2.2 Indicate sources of the information in the system. (Check all that apply.)

Directly from individual about whom the information pertains					
In person	X	Hard copy: mail/fax	X	Online	X
Telephone	X	Email	X		
Other (specify):					

Government sources					
Within the Component	X	Other DOJ components	X	Other federal entities	X
State, local, tribal	X	Foreign	X		
Other (specify):					

Non-government sources					
Members of the public	X	Public media, internet	X	Private sector	
Commercial data brokers					
Other (specify):					

2.3 Analysis: Now that you have identified the information collected and the sources of the information, please identify and evaluate any potential threats to privacy that exist in light of the information collected or the sources from which the information is collected. Please describe the choices that the component made with regard to the type or quantity of information collected and the sources providing the information in order to prevent or mitigate threats to privacy. (For example: If a decision was made to collect less data, include a discussion of this decision; if it is necessary to obtain information from sources other than the individual, explain why.)

Potential threats to privacy that exist in light of the information collected or the sources from which the information is collected include unauthorized access to and use of information regarding individuals associated with ATF's criminal investigations and regulatory inspections. There is also a risk that too much information is being maintained and used in NFOCIS. Due to the nature of law enforcement investigations and regulatory inspections, it is a best practice to collect as much information pertaining to subjects or witnesses in investigations or inspections. Information pertinent to an investigation or inspection may need to be obtained from sources other than the individual, such as other Federal or state agencies. To perform mission related duties, it is necessary to collect PII on individuals, including SSNs. A SSN is generally used when applying for credit or applications for housing, it may also be associated with other information that can assist in law enforcement investigations or regulatory inspections. The SSN can be used when querying other databases in gathering related or associated information to an individual.

To mitigate privacy risks, the NFOCIS case management applications are limited to

authorized personnel who have a need to know basis. Once ATF establishes a need to know basis, all authorized users of NFOCIS must undergo a background check, receive a clearance, and be granted access to ATF systems by ATF's Personnel Security Branch. Furthermore, there are security roles in place to limit access for investigations that are deemed more sensitive than typical criminal investigations. For example, electronic files that contain Grand Jury obtained material are restricted and cannot be accessed unless given permission by the case agent. Also, supervisory review is required to ensure that only authorized records are entered and the information is accurate.

For more information about the security controls that have been applied to NFOCIS that assist in mitigating threats related to the collection of PII, please see the Sections 6.1 and 6.2, below.

Section 3: Purpose and Use of the System

3.1 Indicate why the information in the system is being collected, maintained, or disseminated. (Check all that apply.)

Purpose			
X	For criminal law enforcement activities	X	For civil enforcement activities
	For intelligence activities	X	For administrative matters
X	To conduct analysis concerning subjects of investigative or other interest	X	To promote information sharing initiatives
X	To conduct analysis to identify previously unknown areas of note, concern, or pattern.		For administering human resources programs
X	For litigation		
	Other (specify):		

3.2 Analysis: Provide an explanation of how the component specifically will use the information to accomplish the checked purpose(s). Describe why the information that is collected, maintained, or disseminated is necessary to accomplish the checked purpose(s) and to further the component's and/or the Department's mission.

NFOCIS, and specifically the N-Force and N-Quire applications, are used for criminal law enforcement purposes by Special Agents to collect and document investigative data for a variety of criminal investigations within their jurisdiction. ATF agents also have jurisdiction to investigate arsons with a federal nexus or that meet a federal threshold. Information derived from investigations are memorialized within the NFOCIS applications to manage/oversee the investigative activities and facilitate the production of documents to be used during a prosecution.

ATF IOIs document violations within the legal firearms and explosives industries for administrative and civil enforcement activities by conducting inspections of licensed dealers or permittees. Investigators collect information on licensee activities and violations during those inspections and input them into the N-Spect application within NFOCIS. IOIs rely on this data when completing their reports of inspection and ultimately use the information when denying, suspending, or revoking a license or permit.

NFOCIS is used to collect and document evidentiary leads involving various targets or sources obtained via interviews conducted in the course of a complex investigation. The data collected is analyzed and aggregated by Special Agents, IOIs, and Investigative Research Analysts to develop additional leads or connect individuals or activities previously unknown to one another. As a standard investigative practice, this information is analyzed to reveal connections or widen the scope of investigations, identify individuals for further interviews or follow-up, and identify trends and patterns of criminal activity, such as multi-jurisdiction firearms trafficking. This process can also reveal existing investigations led by other Federal, state, or tribal law enforcement agencies both nationally and internationally and allows deconfliction of those cases. Continued sharing of this information is essential to efficient resource allocation and enhancing ATF's ability to combat violent crime and terrorism.

The data is reviewed for various administrative purposes. One facet of this is to check the compliance of personnel with ATF Directives in order to maintain accountability. This data is used during internal audits of field divisions and offices in order to reveal any weaknesses in the administrative process set forth by ATF. Data is also used to identify the needs of ATF in order to allocate resources to the most needed areas. Identified trends and patterns are used to dictate the strategic management and direction of ATF for future initiatives and projects. N-Force Vault tracks the status of items of property and evidence that are physically held in various ATF secured locations.[6]

NFOCIS is used to collect civil (non-criminal) information related to entities (corporate, single proprietorship, partnership) and the individuals who have control of such entities. In addition, it is used to identify responsible persons who are required to have had completed a criminal background check for possession of explosives. The data collection is stored within the centralized database and can be queried through the applications.

Additionally, ATF receives requests for information from other government entities, such as, but not limited to, the GAO, the Department of Justice (DOJ) Justice Management Division, Congress, the White House, and the general public through Freedom of Information Act requests. These requests translate to queries built to search for the information contained in the database.

---

[6] This property and evidence can be items including, but not limited to, firearms, explosives, currency, drugs, grand jury documents, or electronic surveillance information in the form of compact disks, digital video disks, or external hard drives. These items are normally seized for evidence or forfeiture.

Lastly, in the course of executing on ATF's mission, Special Agents also collect intelligence information connected to illegal trafficking of alcohol, tobacco, firearms, and explosives or crimes that involve violent crime. Though the information, at the time it is collected/received, may not merit the opening of an investigation, ATF retains the information in the event that the information aids in uncovering illegal activities.

3.3 Indicate the legal authorities, policies, or agreements that authorize collection of the information in the system. (Check all that apply and include citation/reference.)

	Authority	Citation/Reference
X	Statute	**(1)** 18 U.S.C., chapter 40 (related to explosives), chapter 44 (related to firearms), chapter 59 (related to liquor trafficking), and chapter 114 (related to trafficking in contraband cigarettes); **(2)** Chapter 53 of the Internal Revenue Code of 1986, 26 U.S.C. chapter 53 (related to certain firearms and destructive devices); **(3)** Chapters 61 through 80, inclusive, of the Internal Revenue Code of 1986, 26 U.S.C. chapters 61–80, insofar as they relate to activities administered and enforced with respect to chapter 53 of the Internal Revenue Code of 1986, 26 U.S.C. chapter 53; **(4)** 18 U.S.C. §§ 1952, 3667, insofar as they relate to liquor trafficking; **(5)** 49 U.S.C. § 80303 and 80304, insofar as they relate to contraband described in section 80302(a)(2) or 80302(a)(5); and **(6)** 18 U.S.C. §§ 1956–1957, insofar as they involve violations of: **(i)** 18 U.S.C. § 844(f) or (i) (relating to explosives or arson), **(ii)** 18 U.S.C. § 922(l) (relating to the illegal importation of firearms), **(iii)** 18 U.S.C. § 924(n) (relating to illegal firearms trafficking), **(iv)** 18 U.S.C. § 1952 (relating to traveling in interstate commerce in aid of racketeering enterprises insofar as they concern liquor on which Federal excise tax has not been paid); **(v)** 18 U.S.C. §§ 2341–2346, 2341–2346 (trafficking in contraband cigarettes); **(vi)** Section 38 of the Arms Export Control Act, as added by Public Law 94-329, section 212(a)(1), as amended, 22 U.S.C. § 2778 (relating to the importation of items on the U.S. Munitions Import

		List), except violations relating to exportation, in transit, temporary import, or temporary export transactions; **(vii)** 18 U.S.C. § 1961 insofar as the offense is an act or threat involving arson that is chargeable under State law and punishable by imprisonment for more than one year; and **(viii)** Any offense relating to the primary jurisdiction of ATF that the United States would be obligated by a multilateral treaty either to extradite the alleged offender or to submit the case for prosecution if the offender were found within the territory of the United States; **(7)** Investigate, seize, and forfeit property involved in a violation or attempted violation within the investigative jurisdiction set out in paragraph (a), under 18 U.S.C. §§ 981, 982; **(8)** Seize, forfeit, and remit or mitigate the forfeiture of property in accordance with 21 U.S.C. 881 and applicable Department of Justice regulations; and **(9)** Subject to the limitations of 3 U.S.C. 301, exercise the authorities of the Attorney General under section 38 of the Arms Export Control Act, 22 U.S.C. § 2778, relating to the importation of defense articles and defense services, including those authorities set forth in 27 CFR part 47.
	Executive Order	
X	Federal Regulation	(1) 27 CFR Parts 447, 478, 479, 555, 646; (2) 28 CFR §§ 0.130 – 0.133; and (3) 28 CFR Part 25.
X	Memorandum of Understanding/agreement	1. DOJ National Data Exchange – for information sharing pilot program 2. Organized Crime Drug Enforcement Task Force (OCDETF) Fusion Center - shared database initiative
	Other (summarize and provide copy of relevant portion)	

3.4 Indicate how long the information will be retained to accomplish the intended purpose, and how it will be disposed of at the end of the retention period. (Reference the applicable retention schedule approved by the National Archives and Records Administration, if available.)

All data is retained for official law enforcement use only. These records are transferred to the National Archives 15 years after the cases are closed. The Request for Records Disposition

Authority, SF-115, Job No. NI-436-03-5 for NFOCIS and its applications, approved 08/19/2004, provides that the Disposition Schedule for records created in the N-Force/N-Quire applications are maintained at ATF for "75 years after the case is closed, or when no longer needed for legal purposes, whichever is later." Subparagraph b(1) states that the Disposition Schedule for records created within the N-Spect application and maintained at ATF for "25 years after completion of inspection, or when no longer needed for [ATF] business, whichever is later."

3.5 Analysis: Describe any potential threats to privacy as a result of the component's use of the information, and controls that the component has put into place to ensure that the information is handled, retained, and disposed appropriately. (For example: mandatory training for system users regarding appropriate handling of information, automatic purging of information in accordance with the retention schedule, etc.)

Potential threats to the information maintained in NFOCIS include unauthorized access and inappropriate use of the information by approved users. Access controls are role dependent, thus mitigating misuse by users. Based upon a person's position, a comparable access role is granted to specific applications (front end) level and at the database (back end) level. In order to gain authorized access to the NFOCIS data, the end user must complete and submit an access application to a first level supervisor for review. Upon approval by the first level supervisor, Information Security Division's (ISD) Operations Security Branch ensures that the user has a valid and active network and email account. A signed "Rules of Behavior" acknowledgement form must be on file for a network ID. The NFOCIS Owner or Designated Security Officer reviews the application. An NFOCIS system administrator creates an application user ID. ISD's Operations Security Branch tasks a contractor database administrator (DBA) to create a database user account and temporary password.

When reviews of ATF programs are performed by external third parties (e.g., DOJ's Office of Inspector General and the annual Chief Financial Officer (CFO) Act review of ATF's Accountability Report and Auditable Financial Statement), the members of the audit teams work with the Office of Professional Responsibility and Security Operations (OPRSO) and ATF's Financial Management Division to obtain reports of performance data from NFOCIS. Users who are found to have misused their authorized access to any systems are subject to disciplinary action. In the course of reviewing the data specific to ATF's mission and programs, the audit teams also provide ATF management with comment regarding their findings specific to the NFOCIS. The NFOCIS Branch has strengthened information security controls as corrective actions following these reviews.

Records are retained in accordance with the National Archives and Records Administration, guidelines and are disposed of by shredding, burning, or by degaussing.

Section 4: Information Sharing

4.1 Indicate with whom the component intends to share the information in the system and how the information will be shared, such as on a case-by-case basis, bulk transfer, or direct access.

Recipient	How information will be shared			
	Case-by-case	Bulk transfer	Direct access	Other (specify)
Within the component	X			
DOJ components	X			
Federal entities	X			
State, local, tribal gov't entities	X			
Public				
Private sector				
Foreign governments	X			
Foreign entities				
Other (specify):				

4.2 Analysis: Disclosure or sharing of information necessarily increases risks to privacy. Describe controls that the component has put into place in order to prevent or mitigate threats to privacy in connection with the disclosure of information. (For example: measures taken to reduce the risk of unauthorized disclosure, data breach, or receipt by an unauthorized recipient; terms in applicable MOUs, contracts, or agreements that address safeguards to be implemented by the recipient to ensure appropriate use of the information – training, access controls, and security measures; etc.)

Potential privacy risks could include access by unauthorized individuals and misuse by individuals with authorized access. These risks are mitigated as detailed below.

Data contained in N-Force is shared frequently as required by DOJ for deconfliction of targets of investigations. This is done in order to limit duplication of efforts and encourage coordination in order to multiply efforts in pursuing federal violators. Non-grand jury data and National Firearms Act information is validated and then filtered for use by the DOJ National Data Exchange (N-DEx) information sharing pilot program and the OCDETF Fusion Center shared database initiative. To reduce the risk of unauthorized disclosure, ATF only exports limited identifying data (e.g., name, date of birth, SSN) to N-DEx and OCDETF. ATF information is to be accessed only for official law enforcement purposes by law enforcement agencies with jurisdiction to investigate the matter in question. This sharing of information occurs every other month. This responsibility is given to limited personnel within ATF.

There is a Memorandum of Understanding (MOU) in place specifying the limitations or guidelines on the appropriate use of information with participants in the N-DEx. There is also an MOU in place between OCDETF and participating agencies governing the security and privacy of the data once it is shared.

PII is at risk when leaving the secure confines of the original data owner. A breach of data could potentially result in PII being disseminated to a public space. Threats to privacy when information is shared are mitigated by the method to how ATF transfers the data to the shared party. A connection to a DOJ secure shared drive has been made with limited access. Access to N-Force is limited to those that have successfully completed a background investigation and are currently assigned as an ATF employee, ATF Task-Force officer, or an ATF contractor. All ATF and non-ATF employee positions are subject to access restrictions based on position held. In instances where an employee is sharing information, such as investigative reports and or operational plans with our law enforcement partners or in prosecution and/or legal proceedings, the information is generally shared through hard-copy only and system access is not required or permitted. All ATF employees must follow the guidelines specified in ATF policy when sharing hard copies, including supervisory approval, a written prohibition on further disclosure without ATF approval, and completing training on handling sensitive information.

ATF does not share the data contained in the N-Spect or N-Quire applications except as permitted by law (e.g., in accordance with the Privacy Act). Some of the data in N-Spect is considered tax information, which is subject to strict disclosure rules. ATF does not share the data contained in N-Force Vault because it is an internal recordkeeping system.

Section 5: Notice, Consent, and Redress

5.1 Indicate whether individuals will be notified if their information is collected, maintained, or disseminated by the system. (Check all that apply.)

X	Yes, notice is provided pursuant to a system of records notice published in the Federal Register and discussed in Section 7. .	
X	Yes, notice is, in part, provided by other means.	Specify how: To the extent NFOCIS contains information contained for regulatory inspections, ATF provides notice when collecting information for regulatory inspections as required by the Privacy Act. This notice is provided on the forms that Federal Firearms Licensees fill out.

X	No, notice is, in part, not provided.	Specify why not: NFOCIS primarily contains information compiled for the purpose of identifying individual criminal offenders and alleged offenders. NFOCIS is not the repository for the initial collection of the information, most of which is exempted from the Privacy Act's individual notice provisions, and the Privacy Act's (j)(2) exemption has also been claimed to exempt that same information in this system from 5 U.S.C. § 552a(e)(3).

5.2 Indicate whether and how individuals have the opportunity to decline to provide information.

X	Yes, individuals have, in part, the opportunity to decline to provide information.	Specify how: In some situations, providing information for regulatory transactions (e.g., transfer of firearms, export of firearms, import of firearms, etc.) is voluntary, such as providing a Social Security number for identity purposes. However, if an individual declines, ATF may not be able to provide the requested service, processing may be delayed, or an application may be denied.
X	No, individuals do not have, in part, the opportunity to decline to provide information.	Specify why not: As stated above, information compiled as part of N-Force for the purpose of identifying individual criminal offenders and alleged offenders is not the repository for the initial collection of the information and thus individuals do not have the opportunity to decline to provide information, especially law enforcement sensitive information.

5.3 Indicate whether and how individuals have the opportunity to consent to particular uses of the information.

	Yes, individuals have an opportunity to consent to particular uses of the information.	Specify how:
X	No, individuals do not have the opportunity to consent to particular uses of the information.	Specify why not: Consent is not generally required for secondary disclosures in the law enforcement context.

5.4 Analysis: Clear and conspicuous notice and the opportunity to consent to the collection and use of individuals' information provides transparency and allows individuals to understand how their information will be handled. Describe how notice for the system was crafted with these principles in mind, or if notice is not provided, explain why not. If individuals are not provided the opportunity to consent to collection or use of the information, explain why not.

ATF provides notice when collecting information for regulatory inspections as required by the Privacy Act. N-Spect primarily contains information compiled for regulatory inspections. ATF focused the Privacy Act Statement on the purpose of collecting the information and how ATF handles the information in order to provide transparency of ATF operations. Privacy Act Statements are available on the form for the individual to read before submitting the form. For example, when applying to become a Federal Firearms Licensee, at the end of ATF Form 7 (5310.12), there is a Privacy Act Statement that explains submittal of applicant's PII is mandatory in order for ATF to determine the eligibility of the applicant to obtain a firearms license, and to determine the ownership of the business, the type of firearms or ammunition to be dealt in, the business hours, the business history, and the identity of the responsible persons in the business. Submission of information for regulatory inspection is sometimes voluntary, however, failure to provide information may result in ATF not being able to provide the requested service, processing may be delayed, or an application may be denied.

ATF does not provide notice in other cases, specifically for collecting information for criminal law enforcement investigations. The N-Force application primarily contains information compiled for law enforcement purposes, such as identifying individual criminal offenders or alleged offenders. Information is gathered, used, transferred and shared among other law enforcement agencies, if necessary, in order to support ATF's law enforcement mission, strategic goals, program initiatives, and tactical field activities. Notice tends to undermine effect use of personal information in many of these law enforcement contexts.

Further, criminal law enforcement information maintained by ATF is exempted from the Privacy Act's individual notice provisions, and the Privacy Act's (j)(2) exemption has been claimed to exempt that same information in this system from 5 U.S.C. § 552a(e)(3). Therefore, no notice is required to be given to subject individuals because the information is collected for law enforcement purposes.

Section 6: Information Security

6.1 Indicate all that apply.

X	The information is secured in accordance with FISMA requirements. Provide date of most recent Certification and Accreditation: The C&A for NFOCIS was completed on 10/01/2013 If Certification and Accreditation has not been completed, but is underway, provide status or expected completion date:
X	A security risk assessment has been conducted.
X	Appropriate security controls have been identified and implemented to protect against risks identified in security risk assessment. Specify: The C&A for the Annual Assessment of DOJ Controls was completed on 04/30/2014.
X	Monitoring, testing, or evaluation has been undertaken to safeguard the information and prevent its misuse. Specify: Continuous Monitoring, System testing and evaluations are accomplished whenever there is a major changed to the system, Annual Assessments, and/or System Assessments for ATO.
X	Auditing procedures are in place to ensure compliance with security standards. Specify, including any auditing of role-based access and measures to prevent misuse of information: Authorized users have specific roles assigned to their user ID that limit them to the data they enter or have specific rights/privileges to address as defined in the procedures. Actual assignments of roles and rules are established as defined in Section 3.5 for obtaining an account. The procedures for creating and maintaining these system accesses are audited regularly and are part of the annual FISMA audit review process. Auditing and system log review, to include weekly audits of user logs to ensure compliance with security and use standards are on-going activities. Additionally, Oracle and system audits are conducted at least monthly to check for vulnerabilities, weak passwords, undocumented system changes, and policy deviations. Account activity is monitored for inactivity and other anomalies. There is a clear separation of duties to prevent any one person from having sufficient access to allow inappropriate access or to work around the controls in place. The possibility of power users or administrators being able to access information inappropriately has been addressed by having forced system and audit logs copied off in real time to a secured logging server where the data is reviewed daily for anomalies. If logs do not arrive as expected, alerts are generated. The intrusion detection systems are monitored for unusual traffic, especially traffic going to the Internet.
X	Contractors that have access to the system are subject to provisions in their contract binding them under the Privacy Act.
X	Contractors that have access to the system are subject to information security provisions in their contracts required by DOJ policy.
X	The following training is required for authorized users to access or receive information in the system:

	X	General information security training
	X	Training specific to the system for authorized users within the Department.
	X	Training specific to the system for authorized users outside of the component.
		Other (specify):

6.2 Describe how access and security controls were utilized to protect privacy and reduce the risk of unauthorized access and disclosure.

Technical and management controls are in place to protect this data. One example of a management control in place is the procedure for an agent to release information outside of ATF. The request and approval or denial must be documented in the form of a memo from the requesting agent to the Special Agent in Charge of the division. Per ATF policy, these documents must be filed to document the release or denial of release of information to entities outside of ATF. This includes release of information to other law enforcement agencies. One example of the technical controls in place is the tracking of access to sensitive information in the database. This acts as a deterrent for anyone who accesses this information with the intent of violating privacy and security protocols.

The appropriate security controls have been identified and implemented to protect against risks identified in the security risk assessment, including but not limited to, security controls for account management, access controls, access privileges, authentication, least privilege, account restrictions, controlled use of administrative privileges, account monitoring and control, authenticator management, audit reviews, analysis, and reporting. These are just some of the security controls that are in place to protect privacy and reduce the risk of unauthorized access and disclosure. Account management's least privileges security controls ensures that there is a clear separation of duties to prevent any one person from having more access to the system than defined by the assigned user role type. Due to the sensitive nature of the information captured, a number of design choices were made to protect the data. The tables are accessed by special purpose limited applications to ensure that someone who may have access to one piece, such as the property tracking aspect, may not have access to other active case data. Additionally, a number of roles were designed to ensure that only the certain subsets of data could be viewed. Logs of user activity are in place as well as careful consideration of the client's interaction with the application further limiting potential user threat to the system.

Users of the system must complete mandatory Information Security Awareness training and sign the Rules of Behavior on an annual basis to maintain network accounts and access to the system.

Section 7: Privacy Act

7.1 Indicate whether a system of records is being created under the Privacy Act, 5 U.S.C. § 552a. (Check the applicable block below and add the supplementary information requested.)

X	Yes, and this system is covered by an existing system of records notice.

	Provide the system name and number, as well as the Federal Register citation(s) for the most recent complete notice and any subsequent notices reflecting amendment to the system: • JUSTICE/ATF-003, "Criminal Investigation Report System," 68 Fed. Reg. 3553 (January 24, 2003); • JUSTICE/ATF-008, "Regulatory Enforcement Record System," 68 Fed. Reg. 3558 (January 24, 2003); and • Other published Government-wide and DOJ-wide System of Records Notices, depending on the nature of information in the communication or collaboration document and how the information is retrieved.
	Yes, and a system of records notice is in development.
	No, a system of records is not being created.

7.2 Analysis: Describe how information in the system about United States citizens and/or lawfully admitted permanent resident aliens is or will be retrieved.

Information about United States citizens and/or lawfully admitted permanent resident aliens may be retrieved by any PII element or combination of elements identified in Section 2.1, above. The system may be queried and accessed when there is a need for agents, investigators, or other personnel to complete their law enforcement, inspection, or administrative duties. NFOCIS allows for identification of potential suspects and witnesses based on limited known information, ATF personnel then analyze the data to develop leads that are then followed to complete their mission.